AA

Encrypting device for guaranteeing communication safety between apparatus

Patent number: CN1170995

Publication date: 1998-01-21

Inventor: MATSUZAKI NATSUME (JP); HARADA SHUNJI (JP); TAEBAYASHI MAKOTO (JP)

Applicant: MATSUSHITA ELECTRIC IND CO LTD (JP)

Classification:

- International: ***H04L9/32;*** **H04L9/32;** (IPC1-7): H04L9/20

- european: H04L9/32

Application number: CN19970114947 19970522

Priority number(s): JP19960126751 19960522

Also published as:

- EP0809379 (A2)
- US6058476 (A1)
- EP0809379 (A3)
- CN1147087C (C)

Abstract not available for CN1170995

Abstract of corresponding document: **EP0809379**

In the first devices, MPU 53 generates random number R1 as challenge data. Random number R3 is generated by first encryption IC 54, and then combined with random number R1, encrypted, and sent to second device 52 as encrypted text C1. When encrypted text C2 is similarly received from second device 52, first encryption IC 54 decrypts C2 and separates the decrypted result into first separated data RR2 and second separated data RR4. The first encryption IC 54 returns the first separated data to second device 52 as response data. MPU 53 compares the first separated data returned from second device 52 with random number R1, and in the event of a match, authenticates second device 52 as a legitimate device. The first encryption IC 54 generates the time-varying data transfer key by combining second separated data RR4 with random number R3, and transfers the digital copyrighted data to second device 52 by using the data transfer key.

---

[19]中华人民共和国专利局

[51]Int.Cl[6]
H04L 9/20

[12] 发明专利申请公开说明书

[21] 申请号 97114947.X

[43]公开日 1998 年 1 月 21 日

[11] 公开号 CN 1170995A

[22]申请日 97.5.22

[30]优先权

[32]96.5.22 [33]JP[31]126751 / 96

[71]申请人 松下电器产业株式会社

地址 日本大阪府

[72]发明人 松崎夏生 原田俊治 馆林诚

[74]专利代理机构 中国专利代理(香港)有限公司

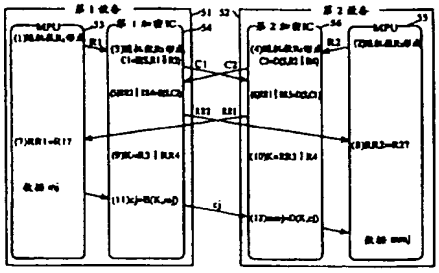
代理人 叶恺东 王忠忠

权利要求书 8 页 说明书 24 页 附图页数 11 页

[54]发明名称 保证设备之间通信安全的加密装置

[57]摘要

在第 1 设备 51 中，MPU53 形成作为询问数据的随机数 R1，第 1 加密 IC54 将上述随机数 R1 和本身形成的数据传送键用的随机数 R3 结合并加密，之后作为密码文字 C1 发送给第 2 设备 52。同样，当接收第 2 设备 52 发送的密码文字 C2 时，第 1 加密 IC54 对上述密码文字 C2 进行译码，将其分成第 1 分离数据 RR2 和第 2 分离数据 RR4。第 1 加密 IC54 将第 1 分离数据 RR2 作为响应数据返回给第 2 设备 52。MPU53 对第 2 设备 52 返回的第 1 分离数据 RR1 和随机数 R1 进行比较，在它们保持一致的场合，认证第 2 设备 52 为正当的设备。



的随机数，以及与实现数据传送件共用的随机数．此外，用于认证的随机数的形成或用于认证的比较处理在加密 IC 内部进行。因此，由于随机数没有按原样在加密 IC 的外部出现，这样，相对以加密 IC 作为译解器的侵入来说，可更加安全。另外，由于上述原因，即使每个随机数的位数较少，仍可保证十分安全。

（第 4 实施例）

下面对第 4 实施例的加密装置进行说明。

该加密装置的目的在于减小加密 IC 的尺寸，其与上述第 1 ～ 3 实施例的不同点在于：它采用单向认证，另外数据传送键处于公开状态。但是，上述实施例以下述条件为前题，该条件为：密码算法 E 和其逆变换算法 D 处于秘密状态。

图 7 表示从第 1 设备 91 向第 2 设备 92 传送数据作品 mj 时的处理程序的示意图。

图 8 为表示第 1 加密 IC94 的硬件结构的方框图。

（ 1 ）首先，第 1 加密 IC94 的随机数形成部 101 形成随机数 R1 ，该随机数 R1 同时用作询问数据和数据传送键，之后，将该随机数 R1 存储于随机数存储部 102 中，通过外部 I/F 部 100 将其发送给第 2 设备 92 。

（ 2 ）第 2 加密 IC96 通过预先与第 1 加密 IC94 共同采用的认证键 S ，对所接收的随机数 R1 进行密码处理，之后将所获得的译码文字 C1 发送给第 1 设备 91 。

（ 3 ）在第 1 加密 IC94 中， E 函数 106 采用认证键 S 对通过外部 I/F 部 100 和开关 105 接收的译码文字 C1 进行加密，该认证键 S 与预先存储于认证键 S 存储部 103 中的上述认证键 S 相同。其结果是，所获得的数据 RR1 通过开关 107 传送给比较部 108 ，在这里，将其与存储于随机数存储部 102 中的随机数 R1 进行比较。

（ 4 ）当比较结果保持一致时，由于第 2 设备 92 可认证为正当的设备，这样，比较部 108 可按照下述方式对开关 104 进行控制，该方式为存储于随机数存储部 102 中的随机数 R1 用作数据传送键。

（ 5 ） E 函数 106 采用通过开关 104 给出的随机数 R1 对数据作品 mj 进行加密，该数据作品 mj 是从 MPU93 通过外部 I/F 部 100 和开关 105 给出的。之

后，通过开关 107 和外部 I/F 部 100 将其发送给第 2 设备 92 。

（ 6 ）在第 2 设备 92 的第 2 加密 IC96 中，以步骤（ 2 ）中所接收的随机数 R1 作为数据传送键，对由第 1 设备 91 给出的数据作品 Cj 进行译码处理，之后将所获得的数据作品 mmj 传送给 MPU95 。

按上述方式，在本实施例中，借助比第 1 ～ 3 实施例少的步骤和组成部件，实现认证、数据传送键的共用、以及数据的密码通信。

另外，在本实施例中，由于从第 1 设备 91 发送给第 2 设备 92 的随机数 R1 按照原样用作数据传送键，这样第 3 者很容易得知数据传送键。但是，即使在得知该数据传送键的第 3 者对数据作品 Cj 进行盗用译码处理的情况下，如上所述，由于密码算法 E 和其逆变换算法 D 处于秘密状态，这样上述尝试不会成功。

另外，即使第 3 者通过伪造合适的随机数 R1 而对密码算法进行译解的情况下，由于仅仅随机数形成部 101 可将新的随机数 R1 存储于随机数存储部 102 中，另外不存在下述的机构，该机构指从上述第 1 加密 IC94 的外部将新的随机数 R1 存储于随机数形成部 101 中，这样上述尝试也不会成功。

按上述方式，如果密码算法和其逆变换算法处于秘密状态，则还可通过本实施例的尺寸较小的加密 IC 实现认证、数据传送键的形成、以及密码通信。

此外，在上述第 1 ～ 4 实施例中，用于在加密 IC 中设定认证键 S （存储）的方法最好按下述方式进行。

即，该方法步骤包括：在加密 IC 制造时预先设定部分认证键 S ，其余的认证键 S 在上述加密 IC 制造后写入。具体地说，认证键 S 存储部的一部分由写入有部分认证键 S 的屏蔽 ROM 构成，剩余的认证键 S 由可程序控制地写入的附加 ROM 构成。

由于在仅仅通过屏蔽 ROM 构成的场合，具有下述的缺点，该缺点为：与由于不通过人工形成最终的加密 IC 而具有安全性的情况相反，很容易通过采用逆向工程的芯片解析对设定值进行解析；另外在仅仅通过附加 ROM 构成的场合，与通过逆向工程难于对设定值进行解析的情况相反，通过人工进行设定，会混入错误，造成不正确，这样需要对上述两种场合中的缺点进行弥补。

作为上述第 1 ～ 4 实施例的密码通信中的密码算法的具体实例，也可采用下面的形式。

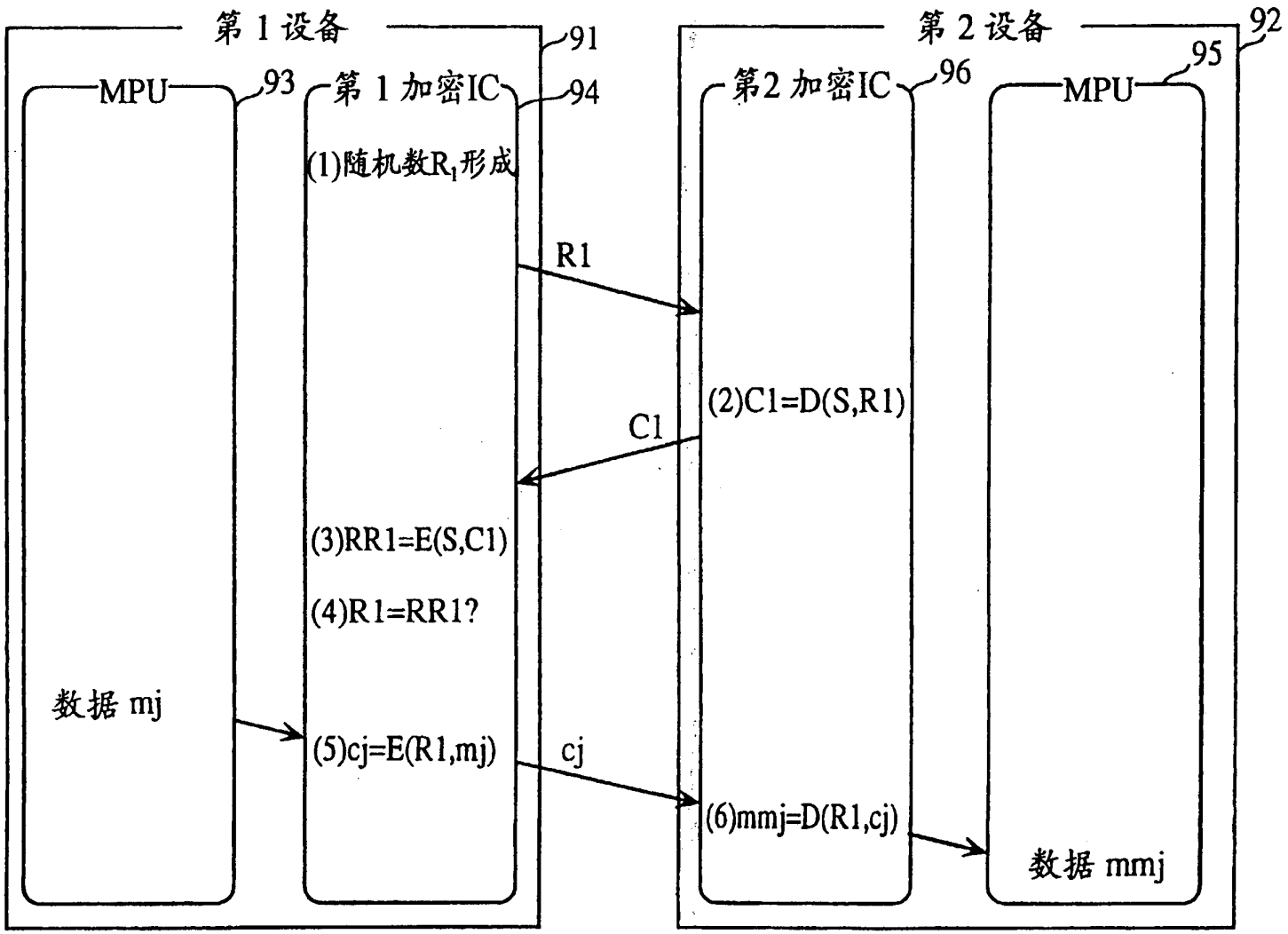

第 1 设备
91
MPU
93
第 1 加密IC
94
(1)随机数R_1形成
R1
(2)C1=D(S,R1)
C1
(3)RR1=E(S,C1)
(4)R1=RR1?
数据 mj
(5)cj=E(R1,mj)
cj
第 2 设备
92
第2 加密IC
96
MPU
95
(6)mmj=D(R1,cj)
数据 mmj

图 7

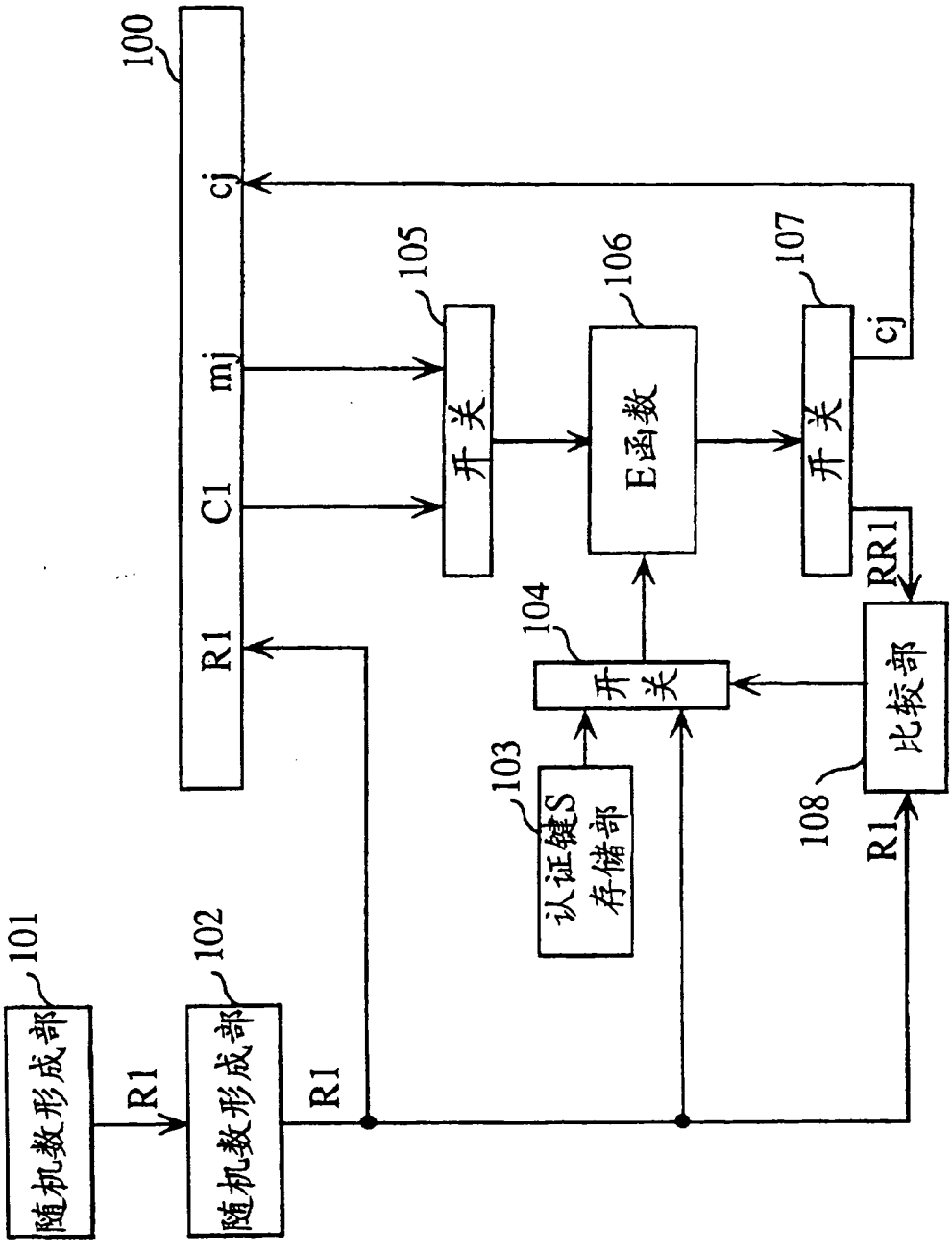

100
cj
mj
C1
R1
105
开关
106
E函数
107
开关
cj
RR1
104
开关
103
认证键S存储部
108
比较部
R1
101
随机数形成部
R1
102
随机数形成部
R1

图 8